

**STATE OF CALIFORNIA  
DEPARTMENT OF INSURANCE  
45 Fremont Street  
San Francisco, California 94105**

File No. RH-01018269

December 4, 2001

**PROPOSED REGULATION TEXT<sup>1</sup>**

*PRIVACY OF NONPUBLIC PERSONAL FINANCIAL  
AND MEDICAL RECORD INFORMATION*

***Table of Contents***

***ARTICLE I.  
GENERAL PROVISIONS***

<i>Section 2689.1.</i>	<i>Authority and Purpose</i>
<i>Section 2689.2.</i>	<i>Scope</i>
<i>Section 2689.3.</i>	<i>Duty of Confidentiality and Care</i>
<i>Section 2689.4.</i>	<i>Definitions</i>

***ARTICLE II.  
PRIVACY NOTICES; OPT OUT NOTICES FOR FINANCIAL INFORMATION***

<i>Section 2689.5.</i>	<i>Initial Privacy Notice</i>
<i>Section 2689.6.</i>	<i>Annual Privacy Notice</i>
<i>Section 2689.7.</i>	<i>Information to be Included in Privacy Notices</i>
<i>Section 2689.8.</i>	<i>Form of Opt Out Notice and Opt Out Methods</i>
<i>Section 2689.9.</i>	<i>Revised Privacy Notices</i>
<i>Section 2689.10.</i>	<i>Delivery of Notices</i>

***ARTICLE III.  
LIMITS ON DISCLOSURES OF MEDICAL RECORD INFORMATION***

<i>Section 2689.11.</i>	<i>Disclosure of Medical Record Information</i>
-------------------------	---

---

<sup>1</sup>. All italicized text is proposed for adoption as new regulation text.

**ARTICLE IV.**  
**STANDARDS FOR SAFEGUARDING NONPUBLIC PERSONAL INFORMATION**

<i>Section 2689.12.</i>	<i>General Provisions</i>
<i>Section 2689.13.</i>	<i>Definitions</i>
<i>Section 2689.14.</i>	<i>Information Security Program</i>
<i>Section 2689.15.</i>	<i>Objectives of Information Security Program</i>
<i>Section 2689.16.</i>	<i>Assess Risk</i>
<i>Section 2689.17.</i>	<i>Manage and Control Risk</i>
<i>Section 2689.18.</i>	<i>Service Providers</i>
<i>Section 2689.19.</i>	<i>Adjust the Program</i>
<i>Section 2689.20.</i>	<i>Enforcement</i>

**ARTICLE V.**  
**ADDITIONAL PROVISIONS**

<i>Section 2689.21.</i>	<i>Protection of Fair Credit Reporting Act</i>
<i>Section 2689.22.</i>	<i>Nondiscrimination</i>
<i>Section 2689.23.</i>	<i>Severability</i>
<i>Section 2689.24.</i>	<i>Effective Date</i>

***Appendix A –Sample Clauses***

## **ARTICLE I. GENERAL PROVISIONS**

### **Section 2689.1      Authority and Purpose**

*The Commissioner promulgates these regulations pursuant to the implied authority granted by California Insurance Code Sections 791 et seq. and 15 U.S.C. Sections 6801(b) and 6805(b) to implement California Insurance Code and Gramm-Leach-Bliley privacy provisions consistent with providing individuals the maximum privacy protections permitted by those laws.*

*NOTE: Authority cited: Sections 791 – 791.27, Insurance Code, 15 U.S.C. Sections 6801, 6805, 6807. Reference: Sections 791 – 791.27, Insurance Code.*

### **Section 2689.2.      Scope**

*These regulations govern the treatment, by all licensees of the California Department of Insurance, of nonpublic personal information (as defined in California Insurance Code Section 791.02(s)) about individuals who obtain or are claimants or beneficiaries of products or services primarily for personal, family, or household purposes. “Nonpublic personal information” includes any list, description or other grouping of consumers (and information pertaining to them which the licensee reasonably believes is lawfully made available to the general public) that is derived using any personally identifiable information that is not publicly available. “Nonpublic personal information” also includes any information about the licensee’s consumer if it is disclosed in a manner that indicates that the individual is or has been the licensee’s consumer; any information the licensee collects through an Internet cookie (an information-collecting device from a web server); and information from a consumer report.*

*If information about individuals associated with a business entity is collected or accessed in connection with a consumer transaction, or is used for marketing products or services intended for personal, family, or household purposes, it is subject to these regulations. Insurance transactions relating to products obtained by a policyholder for business, commercial, or agricultural purposes, but which actually provide insurance primarily for personal, family, or household purposes are subject to these regulations.*

*A dual purpose policy providing only incidental or supplemental commercial coverages is still a policy primarily for personal, family or household purposes and subject to these regulations.*

*Licensees shall also comply with California Civil Code Section 1798.85 (SB 168, Statutes of 2001), Business and Professions Code Sections 17590 through 17595 (SB 771, Statutes of 2001), and all other applicable privacy and confidentiality provisions.*

*NOTE: Authority cited: Sections 791 – 791.27, Insurance Code, 15 U.S.C. Sections 6801, 6805, 6807. Reference: Sections 791.01, 791.02, Insurance Code; Section 1798.85, Civil Code; Sections 17590, et seq., Business and Professions Code; 15 U.S.C. Section 6803.*

### **Section 2689.3.       Duty of Confidentiality and Care**

*Any disclosure of nonpublic personal information shall comply with these regulations and other applicable law, and shall be limited to the minimum amount of personal information necessary to accomplish a lawful purpose. Personal information shall not be disclosed or used in a manner inconsistent with notices provided pursuant to these regulations or other representations made to consumers.*

*NOTE: Authority cited: Sections 791 – 791.27, Insurance Code, 15 U.S.C. Sections 6801, 6805, 6807. Reference: Sections 791.13, Insurance Code.*

### **Section 2689.4.       Definitions**

*As used in these regulations, unless the context requires otherwise:*

*(a)       “Clear and conspicuous” means that a notice is “reasonably understandable” and “designed to call attention to the nature and significance of the information” in the notice. All notices must be clear and conspicuous and accurately reflect the licensee’s privacy policies and practices.*

*A notice is “reasonably understandable” if it:*

- (i)       Presents information in clear, concise sentences, paragraphs, and sections;*
- (ii)      Uses short explanatory sentences (an average of 15 – 20 words) or bullet lists whenever possible;*
- (iii)     Uses definite, concrete, everyday words and active voice whenever possible;*
- (iv)      Avoids multiple negatives;*
- (v)       Avoids legal and highly technical business terminology whenever possible;*
- (vi)      Avoids explanations that are imprecise and readily subject to different interpretations;*
- (vii)     Achieves a minimum Flesch Reading Ease Score of 50; and*
- (viii)    May be understood by those having an average eighth grade educational attainment level.*

*A notice is “designed to call attention to the nature and significance of the information” in it if it:*

- (i)       Uses a plain-language heading to call attention to the notice;*
- (ii)      Uses an easy-to-read typeface and type size (at least 12 point);*

- (iii) *Provides wide margins and ample line spacing;*
- (iv) *Uses boldface or italics for key words;*
- (v) *In a form that combines the licensee's notice with other information, uses distinctive type size, style, and graphic devices, such as shading or sidebars; and*
- (vi) *If on the back or inside of a multi-page form, is accompanied by a prominent notice on the front of the form directing the reader's attention to the privacy notice and where it may be found.*

*A notice on a web site is "designed to call attention to the nature and significance of the information" in it if it is at least 12 point type, uses text or visual cues to encourage scrolling down the page if necessary to view the entire notice and ensure that other elements on the web site (such as text, graphics, hyperlinks or sound) do not distract attention from the notice, and the notice is either:*

- (i) *Placed on a screen that consumers frequently access, such as a page on which transactions are conducted; or*
- (ii) *Accessed from a screen that consumers frequently access through a link that connects directly to the notice and is labeled appropriately to convey the importance, nature and relevance of the notice.*

(b) *"Collect" means to obtain information that the licensee organizes or can retrieve by the name of an individual or by identifying number, symbol or other identifying particular assigned to the individual, irrespective of the source of the underlying information.*

(c) *"Consumer" means an individual who seeks to obtain, obtains or has obtained an insurance product or service from a licensee that is to be used primarily for personal, family or household purposes, and about whom the licensee has nonpublic personal information. "Consumer" includes that individual's legal representative. Examples include, but are not limited to, the following:*

- (i) *An individual who provides nonpublic personal information to a licensee in connection with obtaining or seeking to obtain financial, investment or economic advisory services relating to an insurance product or service, is a consumer regardless of whether the licensee establishes an ongoing relationship.*
- (ii) *An applicant for insurance prior to the inception of insurance coverage is a consumer.*
- (iii) *An individual who is a consumer of another financial institution is not a licensee's consumer solely because the licensee is acting as agent for, or provides processing or other services to, that financial institution.*

*(iv) An individual is a licensee's consumer if the individual is a beneficiary of a life insurance policy underwritten by the licensee, a claimant under an insurance policy issued by the licensee, an insured or an annuitant under an insurance policy or an annuity issued by the licensee, a certificate holder under an employee or other group policy, a personal injury claimant against a commercial liability policy, a worker's compensation claimant, or a mortgagor of a mortgage covered under a mortgage insurance policy; and the licensee discloses nonpublic personal information about the individual to a nonaffiliated third party other than as permitted by California Insurance Code Section 791.13.*

*(v) If the licensee provides initial, annual and revised notices to the plan sponsor, group or blanket insurance policyholder, group annuity contractholder, or workers' compensation plan participant, and does not disclose to a nonaffiliated third party nonpublic personal information about such an individual other than as permitted under California Insurance Code Section 791.13, an individual is not the consumer of the licensee solely because of that relationship. If the licensee does not meet all the conditions of this paragraph, the described individuals are consumers of a licensee.*

*(vi) An individual is not a licensee's consumer solely because he or she is a beneficiary of a trust for which the licensee is a trustee or because he or she has designated the licensee as trustee for a trust.*

*(d) "Customer" means a consumer who has a relationship with a licensee under which the licensee provides one or more insurance products or services to the consumer that are to be used primarily for personal, family or household purposes.*

*A consumer has a continuing relationship with a licensee if the consumer is a current policyholder of an insurance product issued by or through the licensee; or the consumer obtains financial, investment or economic advisory services relating to an insurance product or service from the licensee for a fee.*

*A consumer does not have a continuing relationship with a licensee, and therefore is not a customer, if, for example:*

- (i) The consumer applies for insurance but does not purchase the insurance;*
- (ii) The licensee sells the consumer airline travel insurance in an isolated transaction;*
- (iii) The consumer is no longer a current policyholder of an insurance product or no longer obtains insurance services with or through the licensee;*
- (iv) The consumer is a beneficiary or claimant under a policy and has submitted a claim under a policy choosing a settlement option involving an ongoing relationship with the licensee;*
- (v) The consumer is a beneficiary or a claimant under a policy and has submitted a claim under that policy choosing a lump sum settlement option;*

(vi) *The customer's policy is lapsed, expired, or otherwise inactive or dormant under the licensee's business practices, and the licensee has not communicated with the customer about the relationship for a period of twelve (12) consecutive months, other than annual privacy notices, material required by law or regulation, communication at the direction of a state or federal authority, or promotional materials;*

(vii) *The consumer is an insured or an annuitant under an insurance policy or annuity but is not the policyholder or owner of the insurance policy or annuity; or*

(viii) *The consumer's last known address according to the licensee's records is deemed invalid. An address of record is deemed invalid if mail sent to that address by the licensee has been returned by the postal authorities as undeliverable and if subsequent good faith attempts by the licensee to obtain a current valid address for the individual have been unsuccessful.*

(e) *"Financial institution" means any institution engaged in activities that are financial in nature or incidental to such financial activities as described in Section 4(k) of the Bank Holding Company Act of 1956 (12 U.S.C. 1843(k)).*

*Financial institution does not include:*

(i) *Any person or entity with respect to any financial activity that is subject to the jurisdiction of the Commodity Futures Trading Commission under the Commodity Exchange Act (7 U.S.C. 1 et seq.);*

(ii) *The Federal Agricultural Mortgage Corporation or any entity charged and operating under the Farm Credit Act of 1971 (12 U.S.C. 2001 et seq.); or*

(iii) *Institutions chartered by Congress specifically to engage in securitizations, secondary market sales (including sales of servicing rights) or similar transactions related to a transaction of a consumer, as long as the institutions do not sell or transfer nonpublic personal information to a nonaffiliated third party.*

(f) *"Financial product or service" means any product or service that a financial holding company could offer by engaging in an activity that is financial in nature or incidental to such a financial activity under Section 4(k) of the Bank Holding Company Act of 1956 (12 U.S.C. 1843(k)). Financial service includes a financial institution's evaluation or brokerage of information that the financial institution collects in connection with a request or an application from a consumer for a financial product or service.*

(g) *"Nonaffiliated third party" means any person or entity that is not an affiliate of, or related by common ownership or affiliated by corporate control with, a licensee. Nonaffiliated third party includes any company that is an affiliate solely by virtue of the direct or indirect ownership or control of the company by the licensee or its affiliate in conducting merchant banking or investment banking activities of the type described in Section 4(k)(4)(H) or insurance company investment activities of the type described in Section 4(k)(4)(I) of the federal Bank Holding Company Act (12 U.S.C. 1843(k)(4)(H) and (I)).*

(h) *“Ownership of voting securities,” as used in California Insurance Code Section 790.02(g), means ownership or power to vote twenty-five percent (25%) or more of the outstanding shares of any class of voting security of the person or entity, directly or indirectly, or acting through one or more other persons, and includes power in any manner over the election of a majority of the directors, trustees or general partners (or individuals exercising similar functions) of the person or entity.*

(i) *“Publicly available information” means any information that a licensee has a reasonable basis to believe is lawfully made available to the general public from federal, state or local government records; widely distributed media; or disclosures to the general public that are required to be made by federal, state or local law.*

*A licensee has a reasonable basis to believe that information is lawfully made available to the general public if the licensee has taken steps to determine that the information is of the type that is available to the general public; and when an individual can direct that the information not be made available to the general public, the individual has not done so.*

*NOTE: Authority cited: Sections 791 – 791.27, Insurance Code, 15 U.S.C. Sections 6801, 6805, 6807. Reference: Sections 791.04, Insurance Code; 15 U.S.C. Sections 6801, 6802, 6803, 6809.*

## **ARTICLE II.**

### **PRIVACY NOTICES; OPT OUT NOTICES FOR FINANCIAL INFORMATION**

#### **Section 2689.5. Initial Privacy Notice**

(a) *A licensee shall provide a clear and conspicuous notice that accurately reflects its privacy policies and practices to:*

(1) *A customer, not later than when the licensee establishes a customer relationship, except as provided in subsection (c) of this section; and*

(2) *A consumer, before the licensee discloses any nonpublic personal information about the consumer to any nonaffiliated third party, if the licensee makes a disclosure other than as authorized by California Insurance Code Section 791.13, unless the licensee has a customer relationship with the consumer, or a notice has been provided by an affiliated licensee, the notice clearly identifies all licensees to whom the notice applies, and is accurate with respect to the licensee and the other institutions.*

(b) *When an existing customer obtains a new insurance product or service, the licensee need not provide a new initial notice if the notice most recently provided was accurate with respect to the new insurance product or service.*

(c) *A licensee may provide the initial notice required by subsection (a)(1) within a reasonable time after the licensee establishes a customer relationship if:*

(1) *Establishing the customer relationship is not at the customer's election; for example, if a licensee acquires or is assigned a customer's policy from another licensee or residual market mechanism and the customer does not have a choice about the licensee's acquisition or assignment.*

(2) *Providing notice later than when the licensee establishes a customer relationship would substantially delay the customer's transaction and the customer agrees to receive the notice at a later time; for example, when the licensee and the individual agree over the telephone to enter into a customer relationship involving prompt delivery of the insurance product or service. In that case, the required disclosures and acknowledgements may be given orally, provided that the disclosures are mailed or provided in electronic form within three business days after the sale, and documentation is maintained showing that oral acknowledgement was given by the customer.*

*The customer's transaction is not substantially delayed when the relationship is initiated in person at the licensee's office or through other means by which the customer may view the notice, such as on a web site.*

*NOTE: Authority cited: Sections 791 – 791.27, Insurance Code, 15 U.S.C. Sections 6801, 6805, 6807. Reference: Sections 791.04, Insurance Code; 15 U.S.C. Section 6803.*

#### **Section 2689.6.      *Annual Privacy Notice***

*A licensee shall provide a clear and conspicuous notice to customers that accurately reflects its privacy policies and practices not less than annually during the continuation of the customer relationship. Annually means at least once in any period of twelve (12) consecutive months during which that relationship exists. A licensee may define the twelve-consecutive-month period, but the licensee shall apply it to the customer on a consistent basis. A licensee is not required to provide an annual notice to a former customer with whom it no longer has a continuing relationship.*

*NOTE: Authority cited: Sections 791 – 791.27, Insurance Code, 15 U.S.C. Sections 6801, 6805, 6807. Reference: Section 791.04, Insurance Code; 15 U.S.C. Section 6803.*

#### **Section 2689.7.      *Information to be Included in Privacy Notices***

(a) *The initial, annual and revised privacy notices that a licensee provides under Sections 2689.5, 2689.6, and 2689.9 shall, at a minimum, include each of the following that applies to the licensee and to the consumers to whom the licensee sends its privacy notice:*

(1) *The categories of nonpublic personal information that the licensee collects, from whom and through what techniques the information is collected, the purposes for which it is collected and used, and whether information may be collected from sources other than the consumer;*

- (2) *The categories of nonpublic personal information that the licensee discloses, the circumstances under which disclosures may be made without prior authorization in accordance with the licensee's general business practice, and the purposes for which the information is disclosed, including a statement that medical record information will not be disclosed without signed written consent, except as permitted by law;*
- (3) *The categories of affiliates and nonaffiliated third parties to whom the licensee discloses nonpublic personal information, the types of businesses in which the third parties engage, and the purposes for that disclosure, other than those parties to whom the licensee discloses information under California Insurance Code Section 791.13;*
- (4) *The categories of nonpublic personal information about the licensee's former customers that the licensee discloses and the categories of affiliates and nonaffiliated third parties to whom the licensee discloses nonpublic personal information about the licensee's former customers, other than those parties to whom the licensee discloses information under California Insurance Code Section 791.13;*
- (5) *If, pursuant to California Insurance Code Section 791.13(a), prior written authorization is required before a licensee discloses nonpublic personal information, the written authorization shall comply with the provisions of California Insurance Code Section 791.13(a).*
- (6) *If a licensee discloses nonpublic personal information to a nonaffiliated third party under California Insurance Code Section 791.13(k) (and no other exceptions in California Insurance Code Section 791.13 apply to that disclosure), a separate description of the categories of information the licensee discloses and the categories of third parties to whom the licensee discloses;*
- (7) *If a licensee wishes to disclose or reserve the right to disclose nonpublic personal information to an affiliate for marketing purposes without affirmative authorization or the right to opt out of that disclosure, a statement explaining that information may be disclosed to affiliates for marketing purposes without obtaining prior authorization.*
- (8) *An explanation of the consumer's right to opt out of the disclosure of nonpublic personal information to nonaffiliated third parties, including the methods by which the consumer may exercise that right at that time;*
- (9) *Any disclosures that the licensee makes under Section 603(d)(2)(A)(iii) of the federal Fair Credit Reporting Act (15 U.S.C. 1681a(d)(2)(A)(iii)) regarding the ability to opt out of disclosures of information among affiliates;*
- (10) *The licensee's policies and practices with respect to protecting the confidentiality and security of nonpublic personal information, including a general description as to who is authorized to have access to the information;*

(11) *A statement that the consumer has the right to access and request correction of recorded personal information and a brief description of the manner in which those rights may be exercised; and*

(12) *Any disclosure that the licensee makes under California Insurance Code Section 791.13. A licensee complies with this provision if its notice states that it makes disclosures to other affiliated or nonaffiliated third parties, as applicable, as permitted by law.*

(13) *The statement required by California Insurance Code Section 791.04(b)(5).*

(b) *A licensee does not adequately categorize the information that it discloses if the licensee uses only general terms, such as transaction information about the consumer.*

(c) *If prior authorization is not required and a licensee reserves the right to disclose all of the nonpublic personal information about consumers that it collects, the licensee may simply state that fact without describing the categories or examples of nonpublic personal information that the licensee discloses.*

(d) *An abbreviated notice, as provided for in California Insurance Code Section 791.04(c), shall comply with California Insurance Code Section 791.04(c) and:*

(1) *Be clear and conspicuous;*

(2) *Describe a reasonable means by which the consumer may obtain the notice prescribed by California Insurance Code Section 791.04(b), such as a toll-free telephone number that the individual may call to request the notice or maintaining copies of the notice on hand at the licensee's office that the licensee provides to the individual immediately upon request; and*

(3) *If applicable, contain an opt-out notice complying with these regulations.*

*If the licensee has provided an abbreviated notice and the individual requests more detailed information, the licensee shall provide all reasonably responsive information and not require the individual to make a series of requests. This section does not prohibit the use of multiple links on a website to different categories or levels of information, as long as they are designed to facilitate rather than impede access.*

*NOTE: Authority cited: Sections 791 – 791.27, Insurance Code, 15 U.S.C. Sections 6801, 6805, 6807. Reference: Sections 791.04, 791.05, 791.06, 791.13, Insurance Code.*

#### **Section 2689.8.      *Form of Opt Out Notice and Opt Out Methods***

(a) *If a licensee is required to provide an opt out notice before it shares any nonpublic personal information with a nonaffiliated third party, it shall provide a clear and conspicuous notice to the consumer, with a self-addressed postage paid return envelope, that clearly states in 16-point boldface type "IMPORTANT PRIVACY CHOICES", or similarly highlights the purpose*

*of the notice, so that the consumer may make a decision and provide direction to the licensee regarding the sharing of his or her nonpublic personal information.*

*The notice shall state that the licensee discloses or reserves the right to disclose nonpublic personal financial information about its consumers to nonaffiliated third parties, that the consumer has the right to opt out of that disclosure, and set forth reasonable means by which the consumer may exercise the opt out right.*

*A licensee provides adequate notice that the consumer can opt out of the disclosure of nonpublic personal financial information to a nonaffiliated third party if the licensee provides a notice which complies with California Insurance Code Section 791.06, identifies all of the categories of nonpublic personal financial information which it discloses or reserves the right to disclose, and all of the categories of nonaffiliated third parties to which it discloses the information, and states that the consumer can opt out of the disclosure of that information. The notice shall also identify the insurance products or services that the consumer obtains from the licensee, either singly or jointly, to which the opt out direction would apply.*

*A licensee provides a reasonable means to exercise an opt out right if it designates check-off boxes in a prominent position on the relevant forms with the opt out notice; includes a reply form together with the opt-out notice; provides an electronic means to opt out, such a form that can be sent via electronic mail or a process at the licensee's web site, if the consumer agrees to the electronic delivery of information; or provides a toll-free telephone number that consumers may call to opt out.*

*A licensee does not provide a reasonable means of opting out if, for example, the only means of opting out is for the consumer to write his or her own letter to exercise that opt out right, or the only means of opting out as described in any notice subsequent to the initial notice is to use a check-off box that the licensee provided with the initial notice but did not include with the subsequent notice.*

*(b) If a licensee mails this form with information required by the federal Gramm-Leach-Bliley Act, or other mailing that is not a bill, this form shall be the first page of the mailing. The form required under this section shall include the toll-free telephone number that the licensee sending the form shall establish.*

*If a licensee provides the opt out notice later than required for the initial notice, the licensee shall also include a copy of the initial notice with the opt out notice in writing or, if the consumer agrees, electronically.*

*(c) A licensee is not subject to the notice and opt out requirements for nonpublic personal information if the licensee is an employee or agent of another licensee ("the principal") and:*

*(1) The principal otherwise complies with, and provides the required notices; and*

*(2) The licensee does not disclose any nonpublic personal information to any person other than the principal or its affiliates in a manner permitted by California Insurance Code*

*Sections 791 – 791.27 or these regulations. A licensee not otherwise subject to the notice and opt out requirements for nonpublic personal information is subject to the requirements set forth in California Insurance Code Sections 791 – 791.27 and these regulations if the licensee, prior to issuance of a renewal policy or at any other time, shares nonpublic personal information with any person other than the insurer which issued the existing policy. A licensee shares nonpublic personal information with a person other than the insurer which issued the existing policy if the licensee shares nonpublic personal information with another insurer in an effort to obtain a renewal policy on more favorable terms than the existing policy.*

*(d) When a consumer has declined to exercise the right to opt out in accordance with this section, the nonpublic personal information disclosed pursuant to the consumer’s implied authorization:*

- (1) May not exceed the scope of disclosure stated in the licensee’s opt-out notice;*
- (2) May not include account balance, account number, payment history, or policy number information; and*
- (3) Shall comply with California Insurance Code Section 791.13(k)(1).*

*(e) If two or more consumers jointly obtain an insurance product or service from a licensee, the licensee may provide a single opt out notice, as long as the licensee assumes full responsibility for the accuracy, understandability, and timely delivery of the notice with respect to its own customers, the licensee gives clear and conspicuous notice that the notice is being provided on a joint basis and that individual copies may be obtained upon request, and the consumers have given the licensee a single address of record or the licensee has other reasonable basis to believe that the notice will be adequately communicated to each individual entitled to receive notice.*

*The licensee’s opt out notice shall explain how the licensee will treat an opt out direction by a joint consumer. Any of the joint consumers may exercise the right to opt out. The licensee may either treat an opt out direction by a joint consumer as applying to all of the associated joint consumers or permit each joint consumer to opt out separately. If a licensee permits each joint consumer to opt out separately, the licensee shall permit one of the joint consumers to opt out on behalf of all of the joint consumers. A licensee may not require all joint consumers to opt out before it implements any opt out direction. If one joint policyholder opts out and the other does not, the licensee may only disclose nonpublic personal financial information about the policyholder who opted out and may not disclose information relating to the policyholders jointly.*

*(f) A consumer may exercise the right to opt out at any time. A licensee may share marketing information with nonaffiliated third parties if a consumer does not respond within 45 days of the date the notice was sent. A licensee shall not share information for marketing purposes before the conclusion of the 45-day time period. If a consumer provides an opt-out direction after the licensee has begun sharing nonpublic personal information, the licensee shall comply with the opt-out direction no later than 30 days after the licensee receives it.*

(g) *A consumer's direction to opt out under this section is effective until the consumer revokes it in writing or, if the consumer agrees, electronically.*

*When a customer relationship terminates, the customer's opt out direction continues to apply to the nonpublic personal information that the licensee collected during or related to that relationship. If the individual subsequently establishes a new customer relationship with the licensee, the opt out direction that applied to the former relationship does not apply to the new relationship.*

(h) *Any authorized representative may opt out on behalf of the consumer. A licensee receiving notice that a consumer has opted out shall not require proof of authorization unless it has a reasonable basis for believing that the person submitting the opt-out direction was acting contrary to the wishes of the consumer.*

*NOTE: Authority cited: Sections 791 – 791.27, Insurance Code, 15 U.S.C. Sections 6801, 6805, 6807. Reference: Sections 791.13, Insurance Code; 15 U.S.C. Section 6802.*

#### **Section 2689.9.      Revised Privacy Notices**

*Except as otherwise authorized, a licensee shall not, directly or through an affiliate, disclose any nonpublic personal information about a consumer to a nonaffiliated third party other than as described in the notice provided to that consumer unless:*

- (1) The licensee has provided to the consumer a clear and conspicuous revised notice that accurately describes its policies and practices;*
- (2) The licensee has provided to the consumer a new authorization or opt out form;*
- (3) If prior written authorization is not required, the licensee has given the consumer 45 days to opt out of the disclosure before the licensee discloses the information to the nonaffiliated third party; and*
- (4) The consumer does not opt out.*

*NOTE: Authority cited: Sections 791 – 791.27, Insurance Code, 15 U.S.C. 6801, 6805, 6807. Reference: Sections 791.13, Insurance Code; 15 U.S.C. Section 6802.*

#### **Section 2689.10.      Delivery of Notices**

(a) *A licensee shall provide any required notices, including notices provided at the consumer's request, so that each consumer can reasonably be expected to receive actual notice in writing or, if the consumer agrees, electronically. Notices must be made available in a form capable of retention by the consumer.*

*A licensee may reasonably expect that a consumer will receive actual notice if the licensee:*

- (1) *Hand-delivers a printed copy of the notice to the consumer;*
- (2) *Mails a printed copy of the notice to the last known address of the consumer separately, or in a policy, billing or other written communication;*
- (3) *For a consumer who conducts transactions electronically, posts the notice on the electronic site in accordance with section 2689.4(a) and requires the consumer to acknowledge receipt of the notice as a necessary step to obtaining a particular insurance product or service;*
- (4) *For an isolated transaction with a consumer, such as the licensee providing an insurance quote or selling the consumer travel insurance, posts the notice in a conspicuous location and requires the consumer to acknowledge receipt of the notice as a necessary step to obtaining the particular insurance product or service.*

*A licensee may not reasonably expect that a consumer will receive actual notice of its privacy policies and practices if it:*

- (1) *Only posts a sign in its office or generally publishes advertisements of its privacy policies and practices; or*

- (2) *Sends the notice via electronic mail to a consumer who does not obtain an insurance product or service from the licensee electronically.*

*(b) A licensee may reasonably expect that a customer will receive actual notice of the licensee's Annual Privacy Notice if:*

- (1) *The customer uses the licensee's web site to access insurance products and services electronically and agrees to receive notices at the web site and the licensee posts its current privacy notice continuously in a clear and conspicuous manner on the web site; or*
- (2) *The customer has requested that the licensee refrain from sending any information regarding the customer relationship, and the licensee's current privacy notice remains available to the customer upon request.*

*(c) A licensee may not provide any notice required by these regulations solely by orally explaining the notice, either in person or over the telephone.*

*NOTE: Authority cited: Sections 791 – 179.27, Insurance Code, 15 U.S.C. Sections 6801, 6805, 6807. Reference: Section 791.04, Insurance Code; 15 U.S.C. Sections 6802, 6803.*

**ARTICLE III.**  
**LIMITS ON DISCLOSURES OF MEDICAL RECORD INFORMATION**

**Section 2689.11.      *Disclosure of Medical Record Information***

(a)      *A licensee shall not disclose nonpublic personal medical record information about a consumer to affiliated or nonaffiliated third parties without the consumer’s prior written authorization.*

(b)      *This section does not prohibit, restrict or require an authorization for the disclosure of nonpublic personal medical record information necessary for business, professional or insurance functions pursuant to California Insurance Code Section 791.13.*

*NOTE: Authority cited: Sections 791 – 791.27, Insurance Code, 15 U.S.C. Sections 6801, 6805, 6807. Reference: Section 791.13, Insurance Code.*

**ARTICLE IV.**  
**STANDARDS FOR SAFEGUARDING NONPUBLIC PERSONAL INFORMATION**

**Section 2689.12.      *General Provisions***

*This article establishes standards for developing and implementing administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of nonpublic personal information, pursuant to California Insurance Code Section 791 and sections 501, 505(b), and 507, codified at 15 U.S.C. 6801, 6805(b) and 6807, of GLBA.*

*NOTE: Authority cited: Sections 791—791.27, Insurance Code, 15 U.S.C. Sections 6801, 6805, 6807, 6824. Reference: Section 791, Insurance Code; 15 U.S.C. Sections 6801, 6805, 6807.*

**Section 2689.13.      *Definitions.***

*For purposes of this article, the following definitions apply:*

(a)      *“Customer information systems” means the electronic or physical methods used to access collect, store, use, transmit, protect, or dispose of customer information, whether that information is maintained in paper, electronic, or other form.*

(b)      *“Service provider” means any person or entity that maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to the licensee.*

*NOTE: Authority cited: Sections 791 – 791.27, Insurance Code, 15 U.S.C. Sections 6801, 6805, 6807, 6824. Reference: Section 791, Insurance Code; 15 U.S.C. Section 6827.*

**Section 2689.14. Information Security Program.**

*Each licensee shall implement a comprehensive written information security program that includes administrative, technical and physical safeguards for the protection of customer information. The administrative, technical, and physical safeguards included in the information security program shall be appropriate to the size and complexity of the nature and scope of its activities.*

*NOTE: Authority cited: Sections 791-- 791.27, Insurance Code, 15 U.S.C. Sections 6801, 6805, 6807, 6824. Reference: Section 791, Insurance Code; 15 U.S.C. Section 6825.*

**Section 2689.15. Objectives of Information Security Program.**

*A licensee's information security program shall be designed to:*

- (a) Ensure the security and confidentiality of customer information;*
- (b) Protect against any anticipated threats or hazards to the security or integrity of such information; and*
- (c) Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.*

*NOTE: Authority cited: Sections 791 – 791.27, Insurance Code, 15 U.S.C. 6801, 6805, 6807, 6824. Reference: Section 791, Insurance Code; 15 U.S.C. Section 6825.*

**Section 2689.16. Assess Risk.**

*A licensee shall assess risk. To assess risk, a licensee shall:*

- (a) Identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems;*
- (b) Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of customer information; and*
- (c) Assess the sufficiency of policies, procedures, customer information systems, and other safeguards in place to control risks.*

*NOTE: Authority cited: Sections 791 – 791.27, Insurance Code, 15 U.S.C. Sections 6801, 6805, 6807, 6824. Reference: Section 791, Insurance Code; 15 U.S.C. Section 6825.*

**Section 2689.17. Manage and Control Risk.**

*A licensee shall manage and control risk. To manage and control risk, a licensee shall:*

(a) *Design its information security program to control the identified risks, commensurate with the sensitivity of the information as well as the complexity and scope of the licensee's activities.*

(b) *Train staff, as appropriate, to implement to licensee's information security program; and*

(c) *Regularly test or otherwise regularly monitor the key controls, systems and procedures of the information security program. The frequency and nature of such tests are determined by the licensee's risk assessment.*

*NOTE: Authority cited: Sections 791 – 791.27, Insurance Code, 15 U.S.C. Sections 6801, 6805, 6807, 6824. Reference: Section 791, Insurance Code; 15 U.S.C. Section 6825.*

#### **Section 2689.18. Service Providers**

*A licensee shall oversee service providers. To oversee service providers, a licensee shall:*

(a) *Exercise appropriate due diligence in selecting its service providers; and*

(b) *Require its service providers by contract to implement appropriate measures designed to meet the objectives of this article, and, where indicated by the licensee's risk assessment, takes appropriate steps to confirm that its service providers have satisfied such obligations.*

*NOTE: Authority cited: Sections 791 – 791.27, Insurance Code, 15 U.S.C. Sections 6801, 6805, 6807, 6824. Reference: Section 791, Insurance Code; 15 U.S.C. Section 6825.*

#### **Section 2689.19. Adjust the Program**

*A licensee shall monitor, evaluate, and adjust, as appropriate, its information security program in light of any relevant changes in technology, the sensitivity of its customer information, internal or external threats to information, and the licensee's own changing business arrangements, such as mergers and acquisitions, outsourcing arrangements, and changes to customer information systems.*

*NOTE: Authority cited: Sections 791 – 791.27, Insurance Code, 15 U.S.C. Sections 6801, 6805, 6807, 6824. Reference: Section 791, Insurance Code; 15 U.S.C. Section 6825.*

#### **Section 2689.20. Enforcement**

*The Commissioner shall audit a licensee's compliance with this article in a manner and with such frequency as the Commissioner deems necessary. Violations of this article are subject to California Insurance Code Section 791.15, et seq. and any other enforcement provisions available to the Commissioner.*

*NOTE: Authority cited: Sections 791 – 791.27, Insurance Code, 15 U.S.C. Sections 6801, 6805, 6807, 6824. Reference: Section 791.15, Insurance Code.*

## **ARTICLE V. ADDITIONAL PROVISIONS**

### **Section 2689.21.      Protection of Fair Credit Reporting Act**

*Nothing in these regulations shall be construed to modify, limit or supersede the operation of the federal Fair Credit Reporting Act (15 U.S.C. 1681 et seq.), and no inference shall be drawn on the basis of the provisions of these regulations regarding whether information is transaction or experience information under Section 603 of that Act.*

*NOTE: Authority cited: Sections 791 – 791.27, Insurance Code, 15 U.S.C. Sections 6801, 6805, 6807. Reference: 15 U.S. C. Section 6806.*

### **Section 2689.22.      Nondiscrimination**

*A licensee shall not unfairly discriminate against any consumer or customer because that consumer or customer has opted out from the disclosure of his or her nonpublic personal information pursuant to the provisions of these regulations.*

*A licensee shall not unfairly discriminate against a consumer or customer because that consumer or customer has not granted authorization for the disclosure of his or her nonpublic personal health information pursuant to the provisions of these regulations.*

*As used in this section, “unfairly discriminate” includes denying a consumer or customer a product or service because he or she has not provided the consent required to authorize the financial institution to disclose or share his or her nonpublic personal information.*

*NOTE: Authority cited: Sections 791 – 791.13, Insurance Code, 15 U.S.C. Sections 6801, 6805, 6807. Reference: Section 791.13, Insurance Code.*

### **Section 2689.23.      Severability**

*If any section or portion of a section of these regulations or its applicability to any person or circumstance is held invalid by a court, the remainder of the regulation or the applicability of the provision to other persons or circumstances shall not be affected.*

*NOTE: Authority cited: Sections 791 – 791.27, Insurance Code, 15 U.S.C. Sections 6801, 6805, 6807. Reference: Section 791, Insurance Code.*

### **Section 2689.24.      Effective Date**

*These regulations are effective \_\_\_\_\_ (OAL to insert effective date).*

*Until July 1, 2002, a contract that a licensee has entered into with a nonaffiliated third party to perform services for the licensee or functions on the licensee's behalf need not be amended to include a written requirement that the third party maintain the confidentiality of nonpublic personal information, as long as the licensee entered into the agreement on or before July 1, 2000.*

*NOTE: Authority cited: Sections 791 – 791.27 , Insurance Code, 15 U.S.C. Sections 6801, 6805, 6807. Reference: Section 791, Insurance Code.*

## **APPENDIX A – SAMPLE CLAUSES**

*Licensees, including a group of financial holding company affiliates that use a common privacy notice, may use the following sample clauses, if the clause is accurate for each institution that uses the notice. (Note that disclosure of certain information, such as assets, income and information from a consumer reporting agency, may give rise to obligations under the federal Fair Credit Reporting Act, such as a requirement to permit a consumer to opt out of disclosures to affiliates or designation as a consumer reporting agency if disclosures are made to nonaffiliated third parties.)*

### ***Categories of information a licensee collects***

*A licensee may use this clause, as applicable, to describe the categories of nonpublic personal information it collects.*

*We collect nonpublic personal information about you from the following sources:*

- *Information we receive from you on applications or other forms;*
- *Information about your transactions with us, our affiliates or others; and*
- *Information we receive from a consumer reporting agency.*

### ***Categories of information a licensee discloses***

*A licensee may use these clauses, as applicable, to describe the categories of nonpublic personal information it discloses. A licensee does not adequately categorize the information that it discloses if it uses only general terms such as “transaction information about the consumer.”*

*Alternative 1: We may disclose the following kinds of nonpublic personal information about you:*

- *Information we receive from you on applications or other forms, such as [provide illustrative examples, such as “your name, address, social security number, assets, income, and beneficiaries”];*
- *Information about your transactions with us, our affiliates or others, such as [provide illustrative examples, such as “your policy coverage, premiums, and payment history”]; and*
- *Information we receive from a consumer reporting agency, such as [provide illustrative examples, such as “your creditworthiness and credit history”].*

*Alternative 2: We may disclose all of the information that we collect, as described [describe location in the notice, such as “above” or “below”].*

### ***Categories of information a licensee discloses and parties to whom the licensee discloses***

*A licensee may use this clause, as applicable, to describe the categories of nonpublic personal information about customers and former customers that the licensee discloses and the categories of affiliates and nonaffiliated third parties to whom the licensee discloses.*

*We do not disclose any nonpublic personal information about our customers or former customers to anyone, except as permitted by law.*

***Categories of parties to whom a licensee discloses***

*A licensee may use this clause, as applicable, to describe the categories of affiliates and nonaffiliated third parties to whom the licensee discloses nonpublic personal information.*

*We may disclose nonpublic personal information about you to the following types of nonaffiliated third parties:*

- *Financial service providers, such as [provide illustrative examples, such as “life insurers, automobile insurers, mortgage bankers, securities broker-dealers, and insurance agents”];*
- *Non-financial companies, such as [provide illustrative examples, such as “retailers, direct marketers, airlines, and publishers”]; and*
- *Others, such as [provide illustrative examples, such as “non-profit organizations”].*

*We may also disclose nonpublic personal information about you as permitted by law.*

***Explanation of opt out right***

*A licensee may use this clause, as applicable, to explain the consumer’s right to opt out of the disclosure of nonpublic personal information to nonaffiliated third parties, including the method(s) by which the consumer may exercise that right. The licensee may use this clause if the licensee discloses nonpublic personal information other than as permitted by the exceptions set forth in California Insurance Code Section 791.13.*

*If you prefer that we not disclose nonpublic personal information about you to nonaffiliated third parties, you may opt out of those disclosures, that is, you may direct us not to make those disclosures (other than disclosures permitted by law). If you wish to opt out of disclosures to nonaffiliated third parties, you may [describe, such as “complete and return the Important Privacy Choices for Californians form”].*

***Confidentiality and security***

*A licensee may use this clause, as applicable, to describe its policies and practices with respect to protecting the confidentiality and security of nonpublic personal information.*

*We restrict access to nonpublic personal information about you to [provide an appropriate description, such as “those employees who need to know that information to provide products or services to you”]. We maintain physical, electronic, and procedural safeguards that comply with state and federal regulations to guard your nonpublic personal information.*